



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
|-----------------|-------------|----------------------|---------------------|------------------|

10/723,011

11/26/2003

Vincent J. Zimmer

20002/17853

1136

34431

7590

03/20/2008

HANLEY, FLIGHT & ZIMMERMAN, LLC  
150 S. WACKER DRIVE  
SUITE 2100  
CHICAGO, IL 60606

EXAMINER

HENNING, MATTHEW T

ART UNIT

PAPER NUMBER

2131

MAIL DATE

DELIVERY MODE

03/20/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

|                              |                                       |                                      |  |
|------------------------------|---------------------------------------|--------------------------------------|--|
| <b>Office Action Summary</b> | <b>Application No.</b><br>10/723,011  | <b>Applicant(s)</b><br>ZIMMER ET AL. |  |
|                              | <b>Examiner</b><br>MATTHEW T. HENNING | <b>Art Unit</b><br>2131              |  |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 26 November 2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 November 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>3/9/04, 8/16/06</u> .   | 6) <input type="checkbox"/> Other: _____                          |

1           This action is in response to the communication filed on 11/26/2003.

2                                   **DETAILED ACTION**

3           Claims 1-32 have been examined.

4                                   *Title*

5           The title of the invention is acceptable.

6                                   ***Information Disclosure Statement***

7           The information disclosure statement(s) (IDS) submitted on 3/9/2004, and 8/16/2006 are  
8 in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the  
9 information disclosure statements.

10                                  ***Request for Information under 37 CFR 1.105***

11           Applicant and the assignee of this application are required under 37 CFR 1.105 to  
12 provide the following information that the examiner has determined is reasonably necessary to  
13 the examination of this application.

14           The information is required to enter in the record the art suggested by the applicant as  
15 relevant to this examination in the IDS filed 8/16/2006. Due to the length, 1084 pages, of the  
16 submitted document "Extensible Firmware Interface Specification", the examiner is unable to  
17 provide full consideration of this document. As such, the examiner is requiring the applicant to  
18 provide the specific chapter and section numbers of the document, (i.e. 1.8.4) which relate  
19 directly to subject matter which the applicants believe they have invented (i.e. secure  
20 configuration of a machine in a pre-operating system environment). This information is  
21 reasonably necessary in order for the examiner to be able to give proper consideration to the

submitted document. The applicants are not required to resubmit this document, or any portions thereof.

In responding to those requirements that require copies of documents, where the document is a bound text or a single article over 50 pages, the requirement may be met by providing copies of those pages that provide the particular subject matter indicated in the requirement, or where such subject matter is not indicated, the subject matter found in applicant's disclosure.

This requirement is an attachment of the enclosed Office action. A complete reply to the enclosed Office action must include a complete reply to this requirement. The time period for reply to this requirement coincides with the time period for reply to the enclosed Office action.

### ***Drawings***

The drawings filed on 11/26/2003 are acceptable for examination proceedings.

### ***Specification***

Applicant is reminded of the proper language and format for an abstract of the disclosure.

*The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.*

*The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.*

The abstract of the disclosure is objected to because:

The first sentence "Methods and apparatus...are disclosed" only contains information already available within the title of the invention, and therefore should be removed.

Art Unit: 2132

1 Correction is required. See MPEP § 608.01(b).

2  
3 Brief Summary of the Invention: See MPEP § 608.01(d). A brief summary or  
4 general statement of the invention as set forth in 37 CFR 1.73. The summary is  
5 separate and distinct from the abstract and is directed toward the invention rather  
6 than the disclosure as a whole. The summary may point out the advantages of the  
7 invention or how it solves problems previously existent in the prior art (and  
8 preferably indicated in the Background of the Invention). In chemical cases it  
9 should point out in general terms the utility of the invention. If possible, the  
10 nature and gist of the invention or the inventive concept should be set forth.  
11 Objects of the invention should be treated briefly and only to the extent that they  
12 contribute to an understanding of the invention.

13  
14 The specification is objected to for failing to provide a Brief Summary of the Invention.

15 Correction is required. See MPEP Section 608.01(d)

16  
17 ***Claim Rejections - 35 USC § 112***

18 The following is a quotation of the second paragraph of 35 U.S.C. 112:

19 The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the  
20 subject matter which the applicant regards as his invention.

21  
22 Claims 9-18 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for  
23 failing to particularly point out and distinctly claim the subject matter which applicant regards as  
24 the invention.

25 Claim 9 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for  
26 omitting essential steps, such omission amounting to a gap between the steps. See MPEP  
27 § 2172.01. The claim is directed to "a method of securely configuring a client", however there is  
28 no claim of a step which actually configures a client. Therefore, the claim is missing this  
29 essential step, and is rejected under 35 U.S.C. 112 2nd Paragraph.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

*A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.*

Claims 1- 7, 9-14, 16-17, 19-22, 24-30, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al. (US Patent Number 6,976,163) hereinafter referred to as Hind.

Regarding claims 1 and 26, Hind disclosed a method of securely configuring a first machine (See Hind Fig. 10 Element 706) in a pre-operating system environment (See Hind Col. 2 Paragraph 2), the method comprising: detecting a message (See Hind Col. 11 Lines 19-31); determining an operating mode of the machine (See Hind Col. 12 Lines 45-63); providing an attestation (See Hind Col. 18 Lines 45-52) ; receiving a configuration update (See Hind Col. 18 Lines 52-56); and updating a machine configuration in a pre-operating system environment (See Hind Col. 18 Lines 52-56 and Fig. 11), but Hind failed to specifically disclose performing a shared secret key exchange. However, Hind did disclose decryption at the receiving device using a shared secret (See Hind Col. 3 Lines 52-59).

It would have been obvious to one of ordinary skill in the art at the time of invention to have performed a shared secret key exchange between the firmware distributor and the updatable

Art Unit: 2132

1 device of Hind. This would have been obvious because the ordinary person skilled in the art  
2 would have been motivated to provide both devices with the proper key so that proper encryption  
3 and decryption could occur.

4       Regarding claims 9, and 29, Hind disclosed a method of securely configuring a client  
5 operating in a pre-operating system environment, the method comprising: sending a message  
6 (See Hind Col. 11 Lines 19-31); determining an operating mode of the client machine (See Hind  
7 Col. 12 Lines 45-63); receiving an attestation (See Hind Col. 18 Lines 45-52); verifying the  
8 attestation (See Hind Col. 18 Lines 45-52); and sending a configuration update to the client  
9 machine in a pre-operating system environment (See Hind Col. 18 Lines 52-56), but Hind failed  
10 to specifically disclose performing a shared secret key exchange. However, Hind did disclose  
11 decryption at the receiving device using a shared secret (See Hind Col. 3 Lines 52-59).

12       It would have been obvious to one of ordinary skill in the art at the time of invention to  
13 have performed a shared secret key exchange between the firmware distributor and the updatable  
14 device of Hind. This would have been obvious because the ordinary person skilled in the art  
15 would have been motivated to provide both devices with the proper key so that proper encryption  
16 and decryption could occur.

17       Regarding claim 19, Hind disclosed an apparatus to securely configure a client  
18 machine in a pre-operating system environment, the apparatus comprising: a client machine  
19 comprising: a messaging module configured to detect messages and send messages (See Hind  
20 Col. 11 Lines 19-31); an operating mode (See Hind Col. 12 Lines 45-63); a trusted platform  
21 module configured to provide an attestation (See Hind Col. 18 Lines 45-52); and a configuration  
22 module configured to update the client's configuration in a pre-operating system environment

1 (See Hind Col. 18 Lines 52-56); and a server machine comprising: an messaging module  
2 configured to send messages and receive messages (See Hind Col. 11 Lines 19-31); an  
3 attestation has been verifier (See Hind Col. 18 Lines 45-52); and an update module configured to  
4 generate a client configuration update (See Hind Col. 18 Lines 52-56), but Hind failed to  
5 specifically disclose the client machine comprising a key exchange module configured to  
6 perform a shared secret key exchange, or the server machine comprising a key exchange module  
7 configured to perform a shared secret key exchange after an attestation has been verified.  
8 However, Hind did disclose decryption at the receiving device using a shared secret (See Hind  
9 Col. 3 Lines 52-59).

10 It would have been obvious to one of ordinary skill in the art at the time of invention to  
11 have provided the client and server of Hind each with a shared secret key exchange module.  
12 This would have been obvious because the ordinary person skilled in the art would have been  
13 motivated to provide both devices with the proper key so that proper encryption and decryption  
14 could occur.

15 Regarding claims 2, and 27, Hind disclosed that the message is sent from a second  
16 machine (See Hind Col. 11 Lines 19-31).

17 Regarding claims 3, and 20, Hind disclosed that the operating mode of the first machine  
18 comprises at least one of an IT-managed machine and a consumer machine (See Hind Col. 12  
19 Lines 45-63 and Col. 18 Line 59 – Col. 19 Line 3).

20 Regarding claims 4, 12, and 21, Hind disclosed that the attestation comprises at least one  
21 of machine identity information and a pseudo-anonymous authentication (See Hind Col. 18  
22 Lines 45-52).



1           Regarding claim 5, Hind disclosed that the pseudo-anonymous authentication is provided  
2 by a trusted platform module (See Hind Col. 15 Lines 27-64).

3           Regarding claims 6, and 13, Hind disclosed that the machine identity information  
4 comprises at least one of a serial number, a network name, and a cryptographic representation of  
5 hardware registers (See Hind Col. 18 Lines 45-52).

6           Regarding claims 7, and 14, although Hind did not specifically disclose that the pseudo-  
7 anonymous authentication comprises an Attestation Identity Key, the use of an Attestation  
8 Identity Key is well known to those having ordinary skill in the art, and as such would have been  
9 obvious to employ in the system of Hind for authenticating the client device.

10          Regarding claim 10, Hind disclosed the message is to a client machine (See Hind Col. 11  
11 Lines 19-31).

12          Regarding claim 11, Hind disclosed that the operating mode of the client machine  
13 comprises at least one of an IT-managed device and a personal device (See Hind Col. 12 Lines  
14 45-63 and Col. 18 Line 59 – Col. 19 Line 3).

15          Regarding claims 16, 22, 24, and 28, Hind disclosed that the configuration comprises at  
16 least one of a firmware setting, a BIOS setting, and a machine setting (See Hind Col. 18 Lines  
17 45-52).

18          Regarding claims 17, 25, and 32, Hind did not specifically disclose the configuration  
19 update being encrypted. However, Hind did disclose the update being provided over a network,  
20 and it was well known at the time of invention to encrypt transmissions over a network.  
21 Therefore, it would have been obvious to the ordinary person skilled in the art at the time of  
22 invention to have encrypted the configuration update of Hind. This would have been obvious

1 because the ordinary person skilled in the art would have been motivated to protect the update  
2 from being intercepted by an illicit party.

3       Regarding claim 30, Hind disclosed instructions stored thereon that, when executed,  
4 cause the first machine to send the message via a network connection (See Hind Fig. 10).

5       Claims 8, 18, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind  
6 as applied to claim 1, 9, and 19 above, and further in view of Girard (US Patent Number  
7 7,093,124).

8       Hind disclosed updating BIOS and Firmware in a computer, but failed to specifically  
9 disclose that updating is adapted to operate in an OS-transparent operating mode with  
10 networking support.

11       Girard teaches a system for updating BIOS and system configurations remotely, and  
12 teaches that the use of an agent running in the BIOS, prior to loading the operating system, to  
13 perform authentication of a new boot image and to perform the required configuration, provides  
14 tamper resistance (See Girard Col. 1 Lines 20-47).

15       It would have been obvious to the ordinary person skilled in the art at the time of  
16 invention to employ the teachings of Girard in the firmware updating system of Hind by  
17 performing the downloading, authentication, and configuration of Hind using an agent within the  
18 BIOS which is run prior to loading of the operating system. This would have been obvious  
19 because the ordinary person skilled in the art would have been motivated to provide the updating  
20 with tamper resistance.

21       Claims 15 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind as  
22 applied to claims 9 and 29 above, and further in view of TCPA (Technical Overview for EFI).

1 Hind rendered obvious the use of Attestation Identity Keys for authentication, but failed  
2 to specifically disclose that the attestation is verified by a trusted third party.

3 TCPA teaches that AIKs are obtained through Trusted Third Parties and that the AIKs are  
4 verified by the Trusted Third Party (See TCPA Pages 35-41).

5 It would have been obvious to the ordinary person skilled in the art at the time of  
6 invention to employ the teachings of TCPA in the authentication of the client of Hind by having  
7 a Trusted Third Party verify the AIK. This would have been obvious because the ordinary  
8 person skilled in the art would have been motivated to utilize the AIK system as it was intended  
9 to be used.

10

11

### ***Conclusion***

12

Claims 1-32 have been rejected.

13

The prior art made of record and not relied upon is considered pertinent to applicant's  
14 disclosure.

15

Any inquiry concerning this communication or earlier communications from the  
16 examiner should be directed to MATTHEW T. HENNING whose telephone number is  
17 (571)272-3790. The examiner can normally be reached on M-F 8-4.

18

If attempts to reach the examiner by telephone are unsuccessful, the examiner's  
19 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the  
20 organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/

Examiner, Art Unit 2131

/Gilberto Barron Jr/

Supervisory Patent Examiner, Art Unit 2132